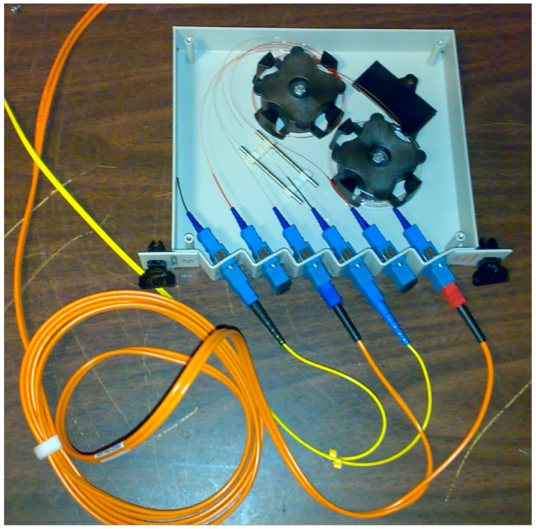
Surveillance, Censorship, and Countermeasures

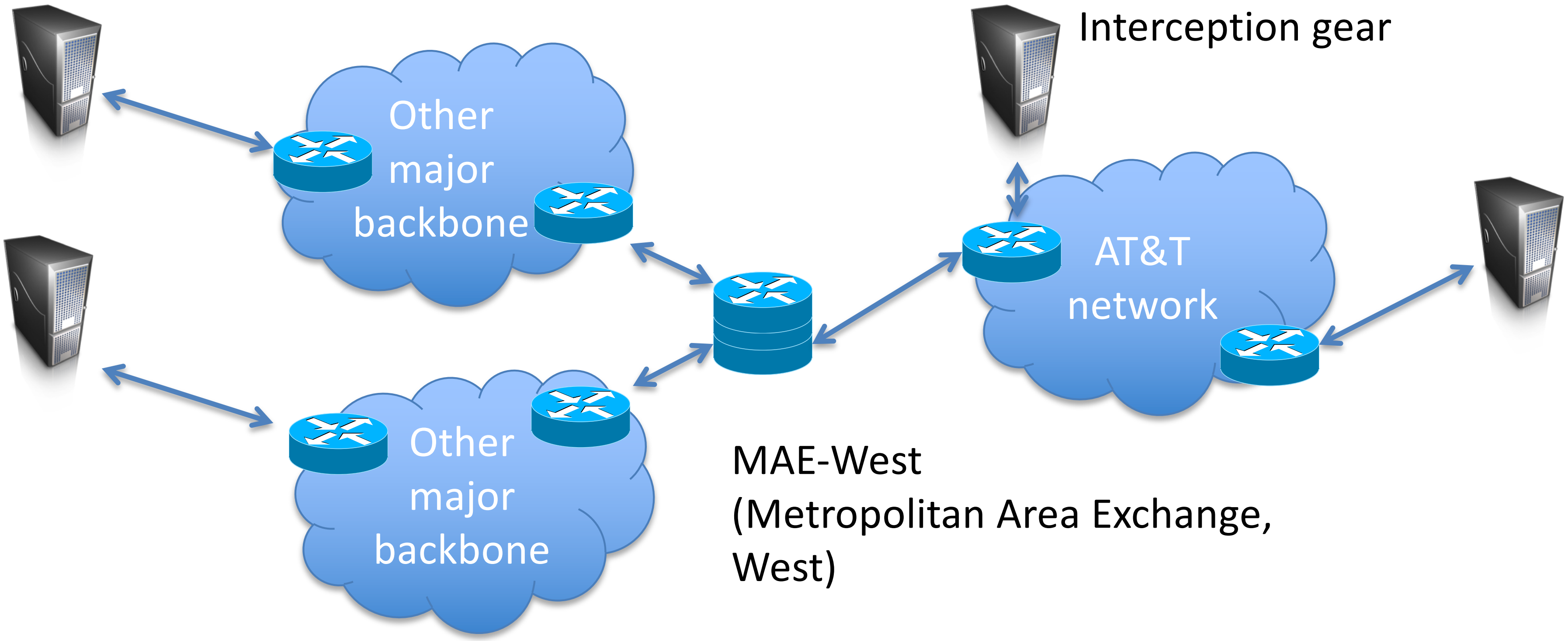
CS642: Computer Security

AT&T Wiretap case

- Mark Klein discloses potential wiretapping activities by NSA at San Francisco AT&T office
- Fiber optic splitter on major trunk line for Internet communications
  - Electronic voice and data communications copied to “secret room”
  - Could read unencrypted webmail
  - Narus STA 6400 device operating at 10 gbps



Wiretap survellaince



Interception gear

Other major backbone

Other major backbone

AT&T network

MAE-West
(Metropolitan Area Exchange,
West)

Large amounts of Internet traffic cross relatively few key points

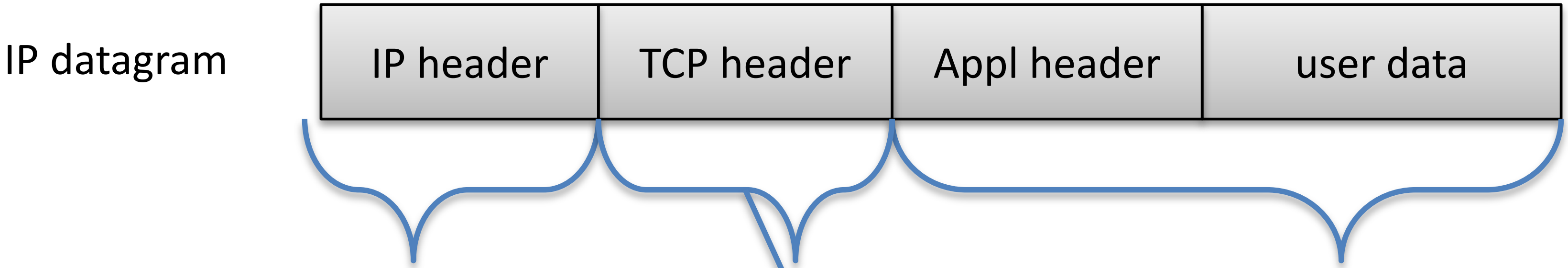
Interception technology

- From Narus website [http://narus.com/index.php/product/narusinsight-intercept]
  - “Target by phone number, URI, email account, user name, keyword, protocol, application and more”, “Service- and network agnostic”, “IPV 6 ready”
  - Collects at wire speeds beyond 10 Gbps

NARUS

BOEING

Types of packet inspection



IP datagram	IP header	TCP header	Appl header	user data

Internet service providers need only look at IP headers to perform **routing**

Shallow packet inspection investigates lower level headers such as TCP/UDP

Deep packet inspection (DPI) analyzes application headers and data

Which inspection is most powerful?

What are the technology challenges?

Lawful intercept

- CALEA
  - Communications Assistance for Law Enforcement Act (1995)
  - Require networks to have built-in surveillance capabilities for targeted collection
- FISA
  - Foreign Intelligence Surveillance Act (1978)
  - Demark boundaries of domestic vs. foreign intelligence gathering
  - Foreign Intelligence Surveillance Court (FISC) provides warrant oversite
  - Executive order by President Bush suspend need for NSA to get warrants from FISC
- Almost all national governments mandate some kind of lawful intercept capabilities

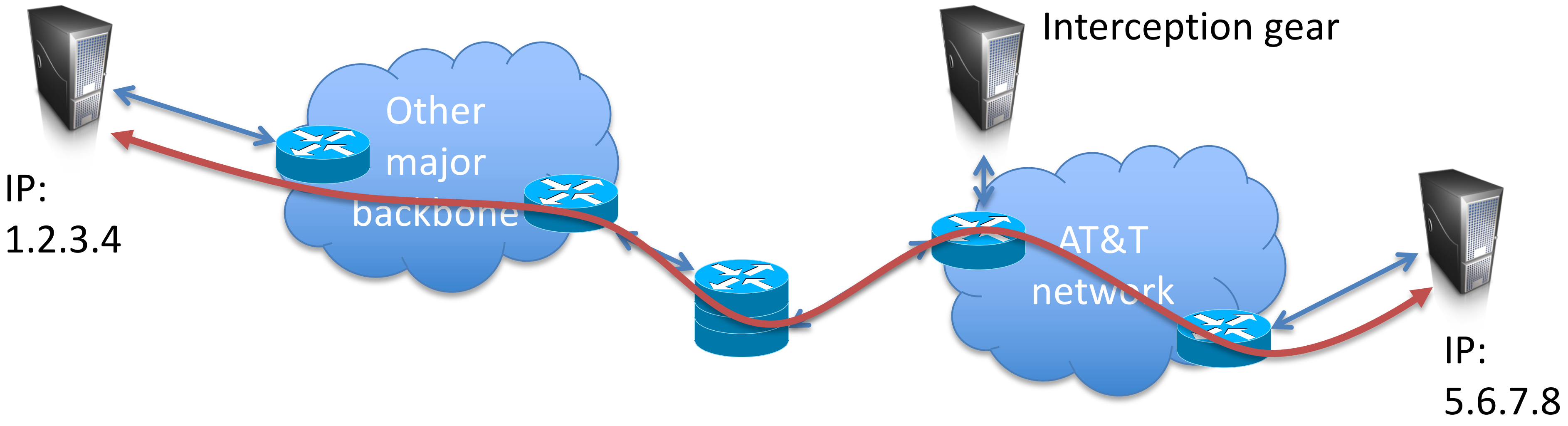
Tension over Surveillance

What are the issues?

1. Do you trust *your* government to use it correctly?
2. Can it be used by anyone else?

Preventing intercept

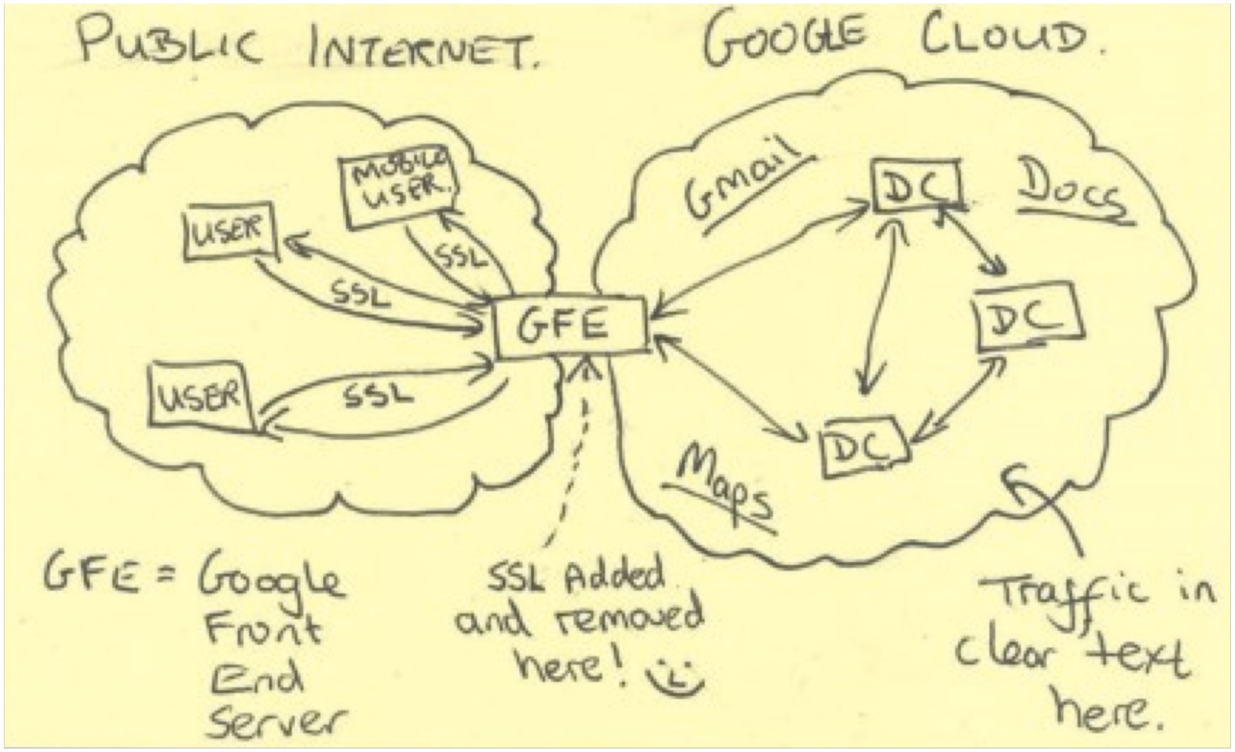
- End-to-end encryption (TLS, SSH)



- What does this protect? What does it leak?
- What can go wrong?

End-run around HTTPS

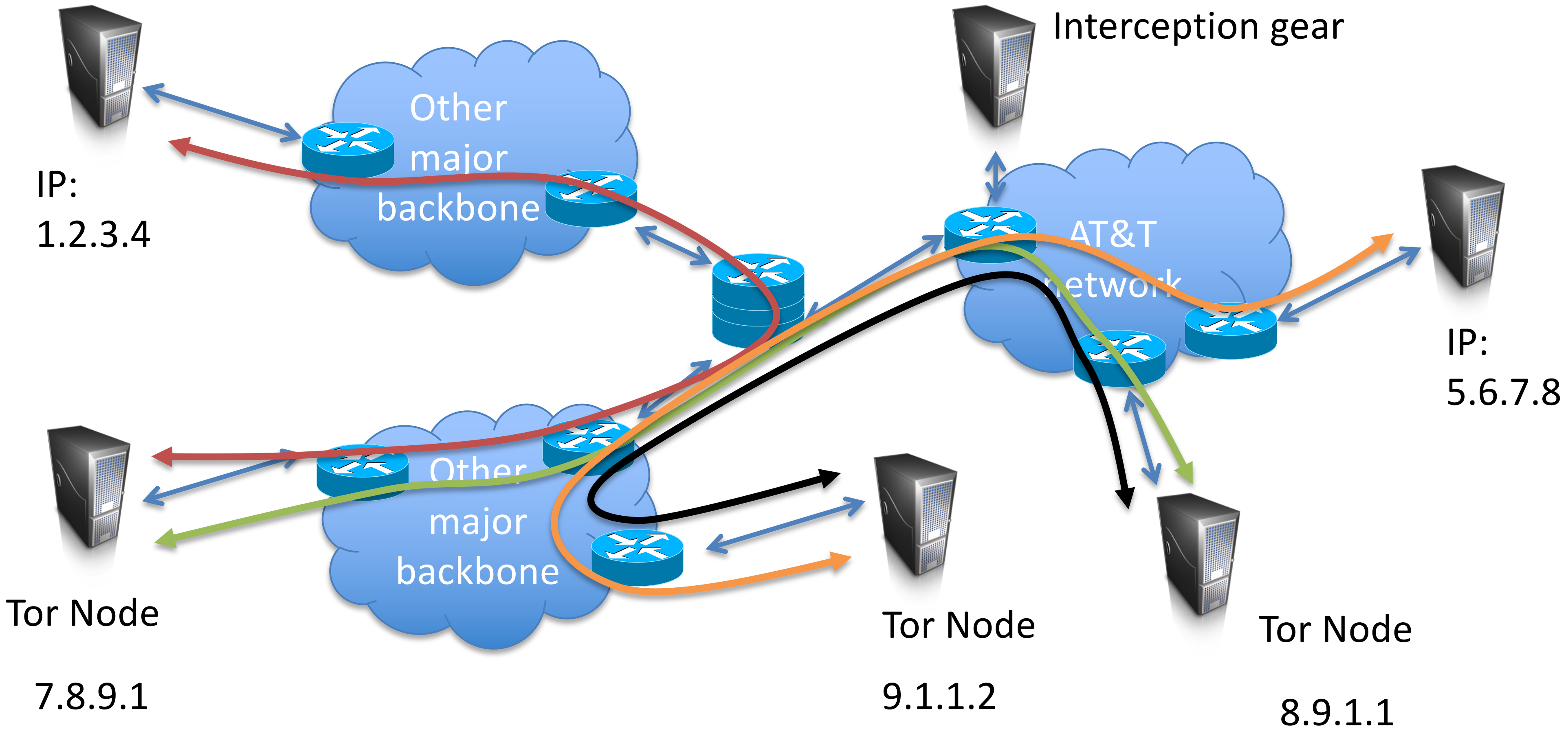
- HTTPS terminated at edge of Google networks
- Internal data center-to-data center communications on privately leased lines
  - No encryption up until last 2013


PUBLIC INTERNET.
GOOGLE CLOUD.
MOBILE USER.
USER
USER
SSL
SSL
SSL
GFE
Gmail
DC
Docs
DC
DC
Maps
GFE = Google Front End Server
SSL Added and removed here! :)
Traffic in clear text here.

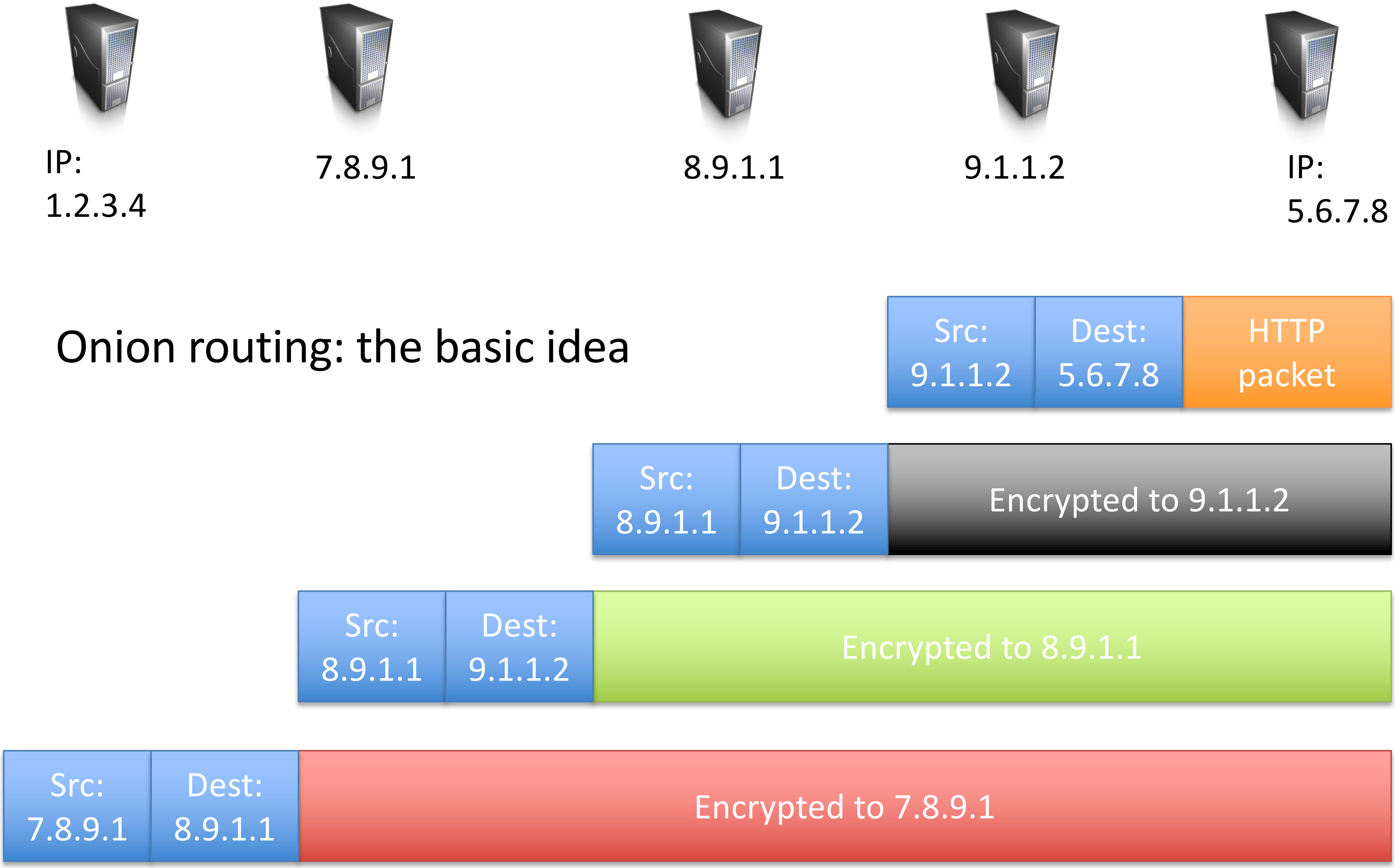
Hiding connectivity is harder

- IP addresses are required to route communication, yet not encrypted by normal end-to-end encryption
  - 1.2.3.4 talked to 5.6.7.8 over HTTPs
- How can we hide connectivity information?

Tor (The Onion Router)



Onion routing: the basic idea



IP:
1.2.3.4

7.8.9.1

8.9.1.1

9.1.1.2

IP:
5.6.7.8

Src: 9.1.1.2 | Dest: 5.6.7.8 | HTTP packet

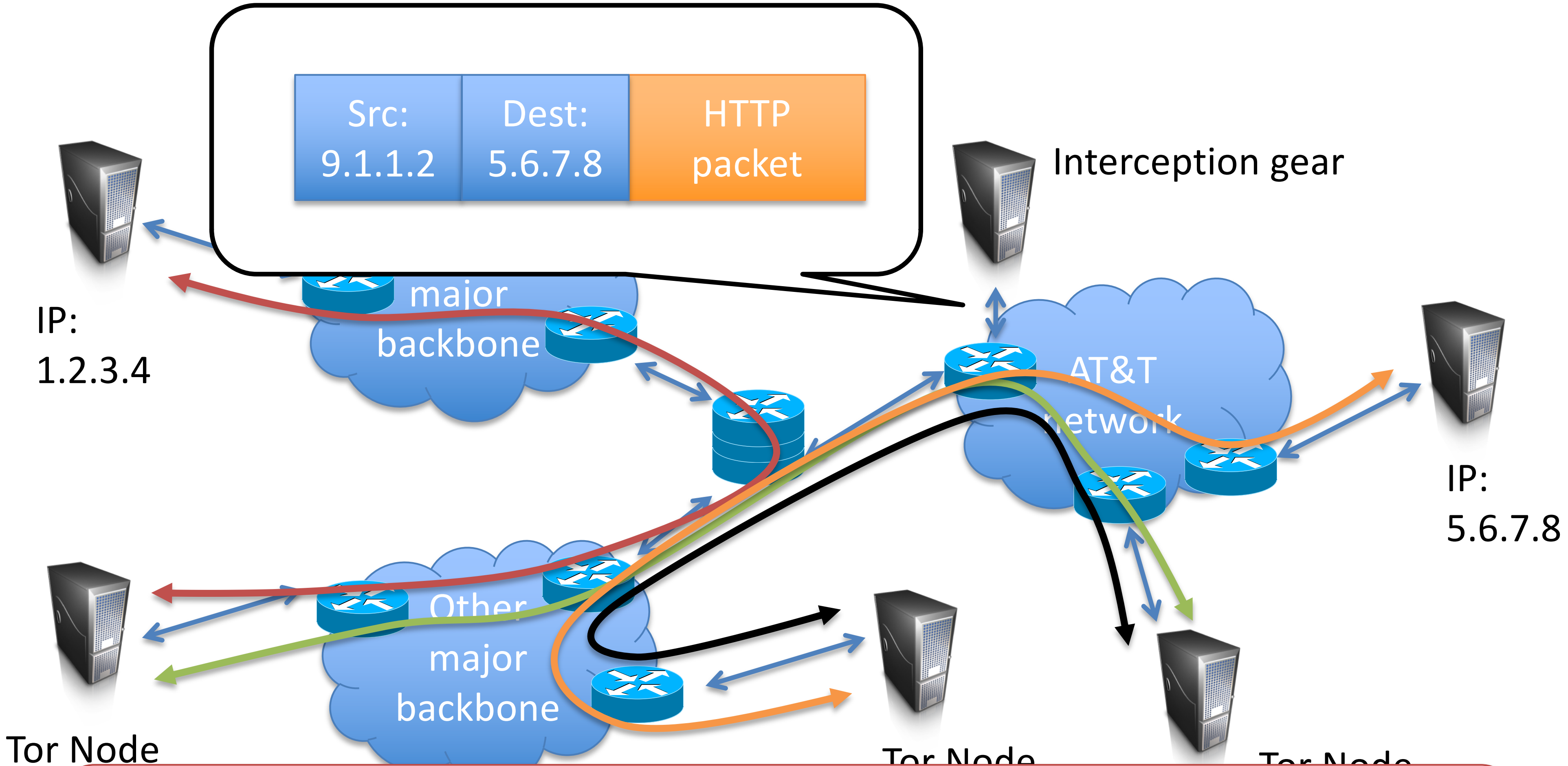
Src: 8.9.1.1 | Dest: 9.1.1.2 | Encrypted to 9.1.1.2

Src: 8.9.1.1 | Dest: 9.1.1.2 | Encrypted to 8.9.1.1

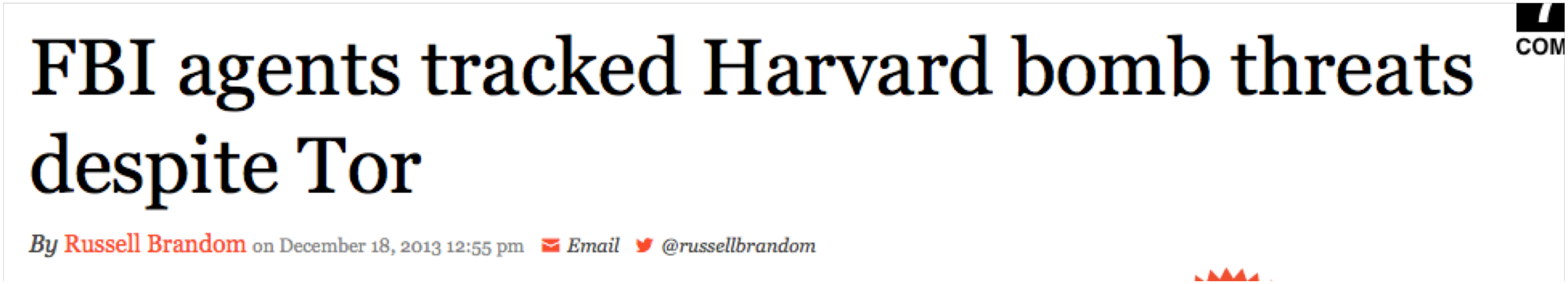
Src: 7.8.9.1 | Dest: 8.9.1.1 | Encrypted to 7.8.9.1

Tor implements more complex version of this basic idea

What does adversary see?



Tor obfuscates who talked to who, need end-to-end encryption (e.g., HTTPS) to protect payload



FBI agents tracked Harvard bomb threats despite Tor

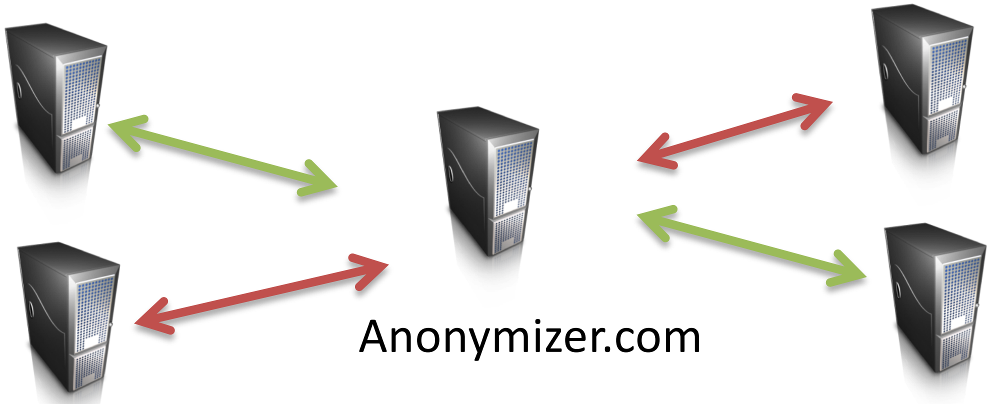
By Russell Brandom on December 18, 2013 12:55 pm ✉ *Email* *@russellbrandom*

- Dec 2016: Eldo Kim, Harvard sophomore, sent bomb threats using Guerilla Mail (anonymous email service)
- Used ToR to connect to Guerilla Mail (from his dorm room)
- Caught within 2 days

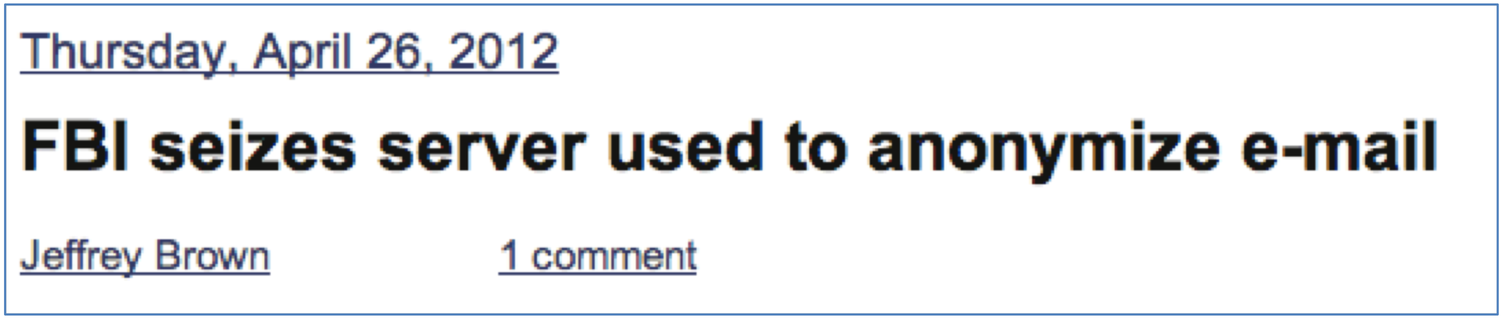
- How did he get caught?
  - Guerilla Mail indicated user connected via ToR node
  - FBI compared timestamp on email to Harvard network logs,
  - He was the only one using ToR at that time, confessed when confronted

Other anonymization systems

- Single-hop proxy services



- JonDonym, anonymous remailers (MixMaster, MixMinion), many more…



Thursday, April 26, 2012

FBI seizes server used to anonymize e-mail

Jeffrey Brown 1 comment

Surveillance via third-party

- “Thus, some Supreme Court cases have held that you have no reasonable expectation of privacy in information you have "knowingly exposed" to a third party — for example, bank records or records of telephone numbers you have dialed — even if you intended for that third party to keep the information secret. In other words, by engaging in transactions with your bank or communicating phone numbers to your phone company for the purpose of connecting a call, you’ve "assumed the risk" that they will share that information with the government.”

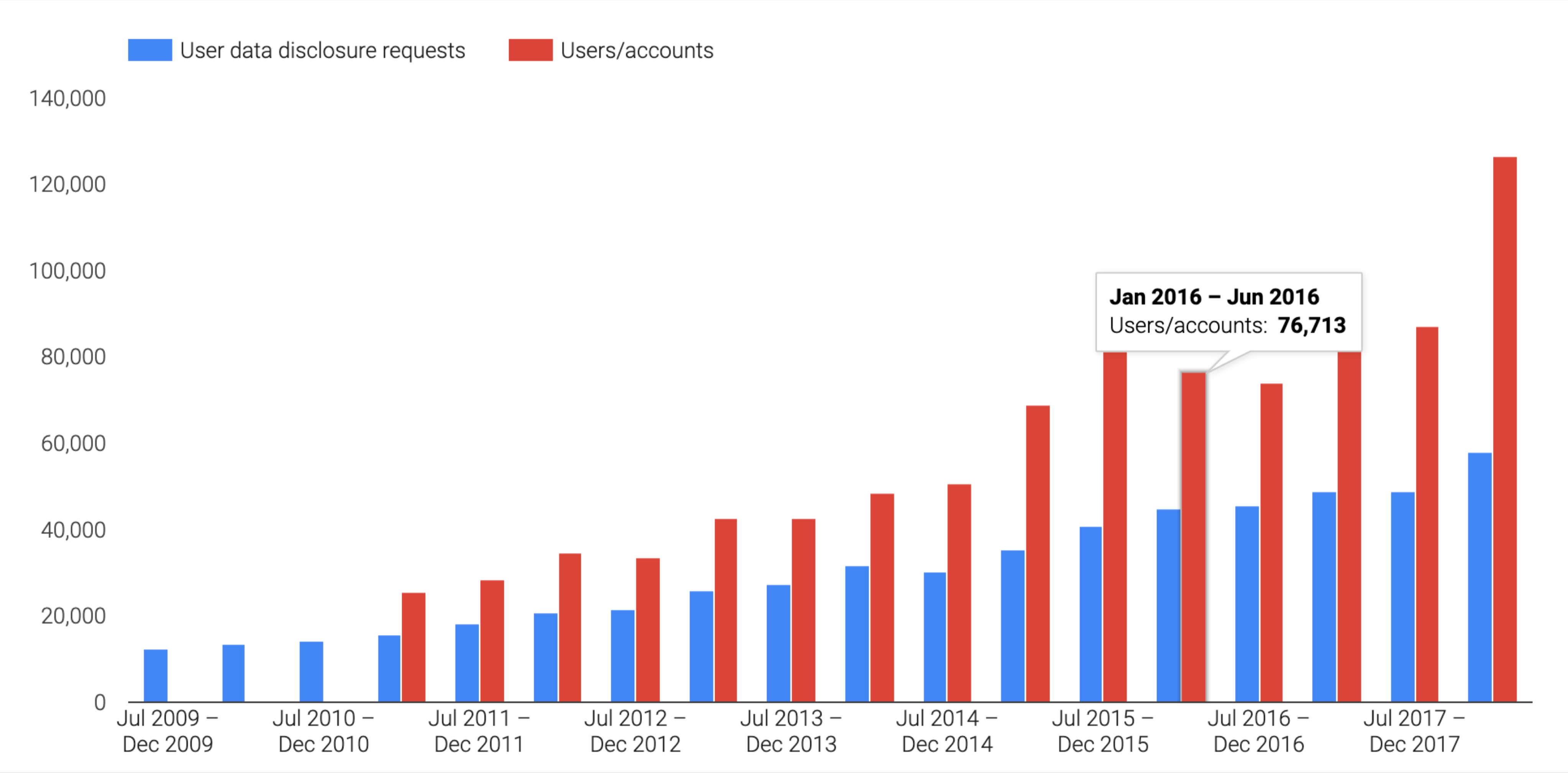
From the EFF website

https://ssd.eff.org/your-computer/govt/privacy

Example: AT&T Hawkeye database

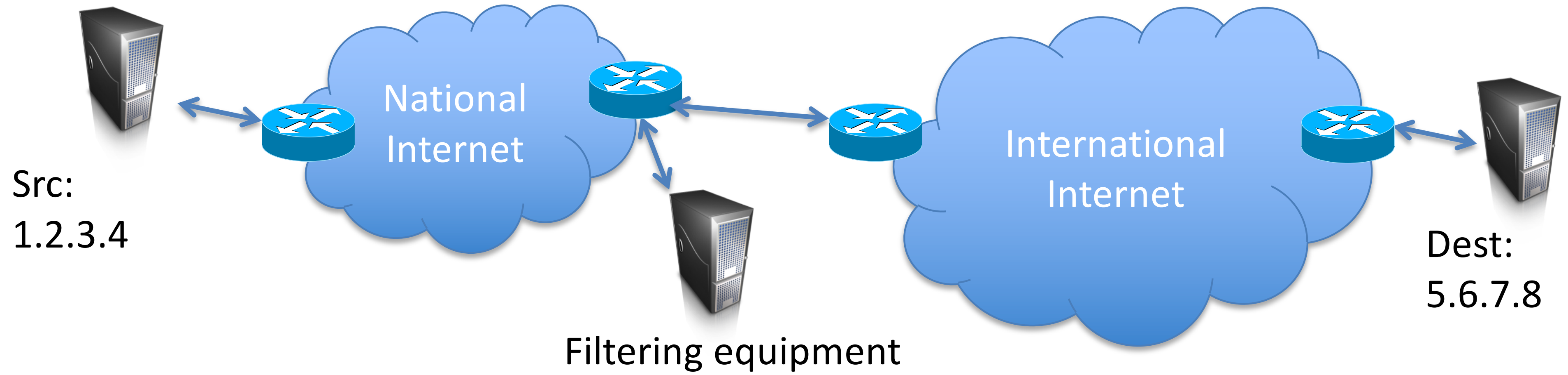
- All phone calls made over AT&T networks since approximately 2001--2006
  - Originating phone number
  - Terminating phone number
  - Time and length of each call

Example: Google data requests



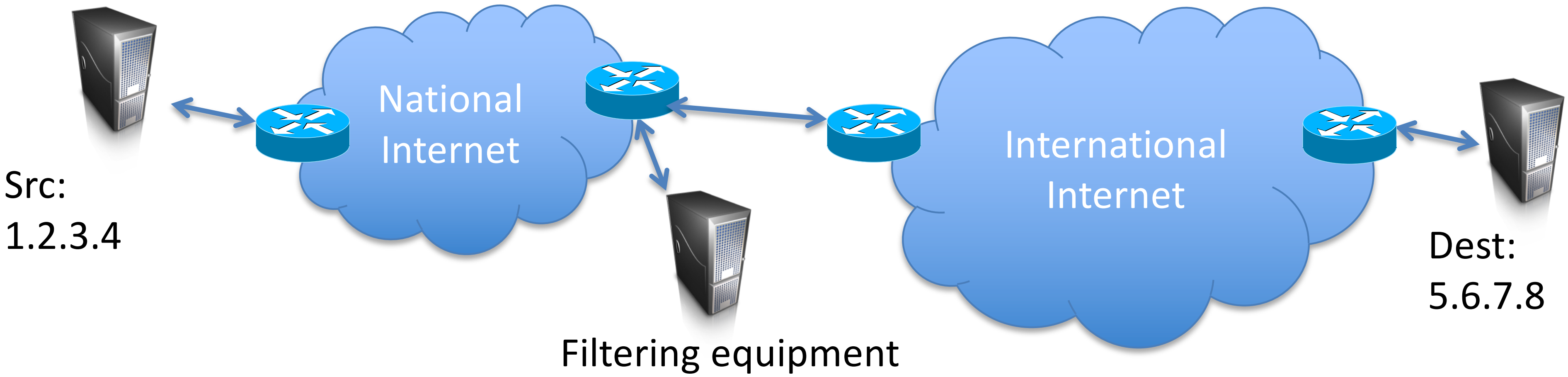
From http://www.google.com/transparencyreport/governmentrequests/userdata/

Censorship via Internet filtering



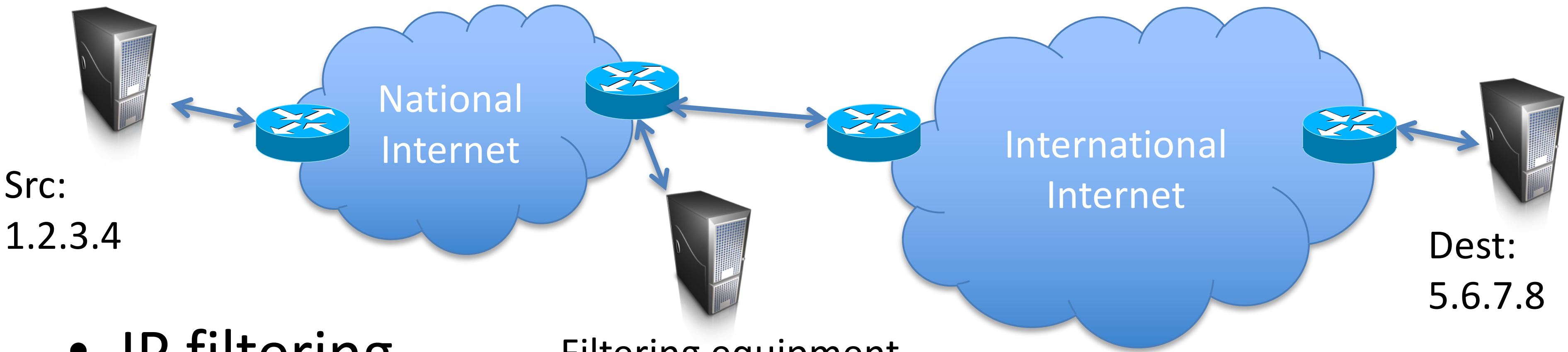
- Golden Shield Project most famous example
- But many other nations perform filtering as well including
  - China
  - Saudi Arabia
  - Belarus

Filtering



- IP filtering
- DNS filtering / redirection
- URL filtering
- Packet filtering (search keywords in TCP packets)
- Protocol filtering (detect Tor protocol)

Circumvention of filtering



- IP filtering
  - Proxies
- DNS filtering / redirection
  - DNS proxy
- URL filtering   or Packet filtering
  - Encryption / Tunneling / obfuscation
- Protocol filtering
  - Obfuscation techniques

Golden Shield Project (Great Firewall of China)

- IP filtering
- DNS filtering / redirection
- URL filtering
- Packet filtering (search keywords in TCP packets)
  - Send TCP FIN both ways
- Protocol filtering (Tor is shut down)

Should we prevent? Can we?

- One can encrypt data that is stored, but no current way to protect data that needs to be used
- Companies are increasingly worried about perception of government surveillance
- Policy?
- Legal protections?